DHHS POLICIES AND PROCEDURES

Section:	**VIII - Privacy and Security Office**
Title:	**NC DHHS - International Travel Policy**
Current Effective Date:	**March 1, 2026**
Revision History:	
Original Effective Date:	**March 1, 2026**

Purpose

The purpose of this policy is to establish risk-based safeguards governing international travel and system access from outside of the United States to protect state-owned systems, state personnel and sensitive data from elevated cybersecurity, surveillance, sanctions, detainment and nation-state threat risks.

The intended outcome of this policy is to:

- Prevent unauthorized or high-risk foreign access to state systems
- Reduce the likelihood of data compromise involving any sensitive and confidential state information included but not limited to Protected Health Information (PHI), Personally Identifiable Information (PII), Federal Tax Information (FTI), etc.
- Ensure compliance with applicable Federal, and North Carolina information security requirements
- Provide clear governance and enforcement standards related to international travel and system use

Policy

This policy is implemented pursuant to Federal and State risk management, access control requirements such as the HIPAA Security Rule (45 CFR §§164.308 and 164.312), NIST SP 800-53 (including AC-17, AC-19, AC-20, SI-4, and CM-7), CMS MARS-E and Acceptable Risk Safeguards (ARS), N.C.G.S. §143B-1376, and the State's International Travel Policy (SCIO-SEC-320). These authorities collectively require risk-based safeguards to protect systems containing sensitive and confidential state information included but not limited to PHI, PII, FTI, etc.

1. International Travel

- International travel means physical travel outside the United States, regardless of:
  - Whether the travel is personal or official; and
  - Whether the individual intends to access State systems.

1.1 Individuals traveling internationally for personal reasons who will not:

- Access State systems.

- Carry Department-issued devices; or
- Conduct Department business

are not subject to approval requirements under Section 2.

However, such individuals shall not:

- Access Federal, State, and Department systems while outside the United States.
- Use personal devices to conduct Federal, State, and Department's business while outside the United States.
- Access cached or synchronized Federal, State, and Department's data while outside the United States; or
- Store or use Federal, State, and Department systems credentials for remote access from outside the United States.

1.2 Conduct of Department Business While Internationally Located
No individual should conduct Federal, State, and Department's business while physically located outside the United States unless prior approval has been granted in accordance with Section 2.

Prohibited activities without prior approval include but are not limited to:

- Accessing Department's email; (Required to uninstall all State/ Department applications on personal devices)
- Participating in virtual meetings related to Department business.
- Transmitting Federal, State, and Department's data.
- Accessing Federal, State, and Department's applications or databases; and
- Discussing sensitive, confidential Federal, State, and Department's systems matters using communication platforms.

These restrictions apply regardless of device type.

1.3 Official international travel that is conducted on behalf of the Department for authorized business purposes, including but not limited to meetings, conferences, site visits, oversight activities, or official engagements are required to seek approval as outlined in subsection 2.

2. Advance Notification and Approval
Any individual who has a need to work while outside the United States must submit a formal Security Exception Form C at least six (6) weeks prior to travel departure date. This requirement applies in the following situations:

- Accessing Federal, State, and Department systems from outside the United States.
- Carrying Department-issued equipment outside the United States.
- Conducting Department business while physically located outside the United States.

The Security Exception Form C request shall include:

- Supervisor's approval.
- Division Director approval.
- Documented business justification.
- Explanation of operational necessity for system access.

- Explanation of why duties cannot reasonably be delegated.
- Review by the Division Information Security Official (ISO); and
- Final approvals by the NC DHHS Chief Deputy Secretary, Chief Information Security Officer (CISO), Chief Information Officer (CIO), and the State CISO and CIO.
- Failure to provide required advance notification may result in denial of system access during travel.

Approval is not automatic and may be denied based on risk assessment.

3. International Travel Requirements

- All international travel requires advance approval in accordance with Section 2.
- Only restricted travel-only (loaner) devices may be issued for approved international travel.
- Standard production devices shall not be taken internationally.

Travel (loaner) devices shall:

- Not contain locally stored sensitive data.
- Be configured with minimum functionality.
- Be subject to inspection upon return; and
- Be fully reimaged upon return.

4. Network and System Access Controls

Access to Federal, State, and Department systems from outside the United States is subject to enhanced security controls and monitoring.

The Department may implement:

- Geolocation-based access restrictions.
- Conditional access controls.
- Multifactor authentication requirements.
- Device compliance validation.
- Session monitoring.
- Functional restrictions based on risk.
- Unauthorized foreign-origin login attempts will result in account suspension pending review.
- Access from outside the United States is not permitted unless explicitly authorized in accordance with this policy.

5. Monitoring & Enforcement

- Geolocation blocking shall be enforced.
- Unauthorized login attempts from outside of the United States will result in automatic account suspension.
- Devices returning from approved travel may be subject to inspection and reimaging.
- Failure to comply with the requirements established within this policy may result in disciplinary action, termination, or personal legal consequences

6. High-Risk Countries

High-risk country designations are based on current homeland security determinations as identified on the websites below:

- U.S. Office of Foreign Assets and Control Sanctions Programs and County List
- Federal threat advisories and alerts - including DHS/CISA alerts

No exceptions or work authorizations will be granted for official international travel to high-risk countries.

7. Effective Date
This policy is effective March 1, 2026 and applies to all NC DHHS employees, contractors, third parties, and any others with access to state systems.

Definitions

A. **High-Risk Country:**
A foreign jurisdiction designated based on documented risk assessment, federal threat advisories, sanctions status, intelligence-informed threat analysis, legal environment risks, or other enterprise security considerations.

B. **Department Business:**
Any activity conducted on behalf of the Department, including but not limited to accessing systems, reviewing or transmitting Federal, State, and Department information, participating in meetings, phone calls, messaging, decision-making, or discussing confidential matters related to Department operations.

C. **Department Information:**
Any data created, received, maintained, or transmitted by the Department, including but not limited to PHI, PII, FTI, any sensitive, confidential state information, internal communications, credentials, system documentation, and operational data.

D. **Access:**
Any attempt to authenticate to, log into, retrieve, transmit, store, sync, or otherwise interact with Federal, State, and Department systems or information, whether through Department-issued or personal devices.

E. **State-Issued Device:**
Any laptop, mobile phone, tablet, removable storage media, or other hardware owned, managed, or configured by the Department or State for official use.

F. **Personal Device:**
Any non–state-issued device capable of accessing or storing Department information,

including devices used to access O365, email, cloud storage, or password managers containing Department credentials.

G. **Official Travel:**
Travel conducted for authorized Department business purposes with prior management approval.

H. **Personal Travel:**
Travel conducted for non-business purposes.

I. **Physical Presence:**
Being physically located within the geographic boundaries of a foreign country, including temporary stays, extended stays, or business travel.

The rest of this page intentionally left blank

Appendix A - Approval Flow Diagram:

Personnel who intend to travel outside the United States for official State business are required to submit a Security Exception Request (Form C) to the North Carolina Department of Information Technology (DIT) prior to removing any State-owned device from the country.

All required fields in Form C must be fully completed, and the Division Director's signature must be obtained before the request is submitted to the Division ISO. Once finalized, the ISO will submit the form to DIT.

Upon receipt, DIT will enter the request into the Ariba system, which will automatically route the submission through the established approval workflow. Designated approvers will receive system-generated notifications and are responsible for reviewing and acting upon the request.

An approval-flow diagram is provided below for reference.

Appendix B – Form C Exception Document

Prior to submitting a Form C Exception to request an international travel authorization please ensure you have reviewed the International High Risk Travel Countries:

- U.S. Office of Foreign Assets and Control Sanctions Programs and County List
- Federal threat advisories and alerts - including DHS/CISA alerts

No travel authorizations will be approved for countries identified on the High Risk Travel document.

For questions or clarification on any of the information contained in this policy, please contact the policy owner or designated contact point: ***NC DHH PSO Policy Coordinator****.*